RXHUB℠

Where the Prescribing Industry Connects

Electronic Prescribing of Controlled Substances
Technical Framework Panel

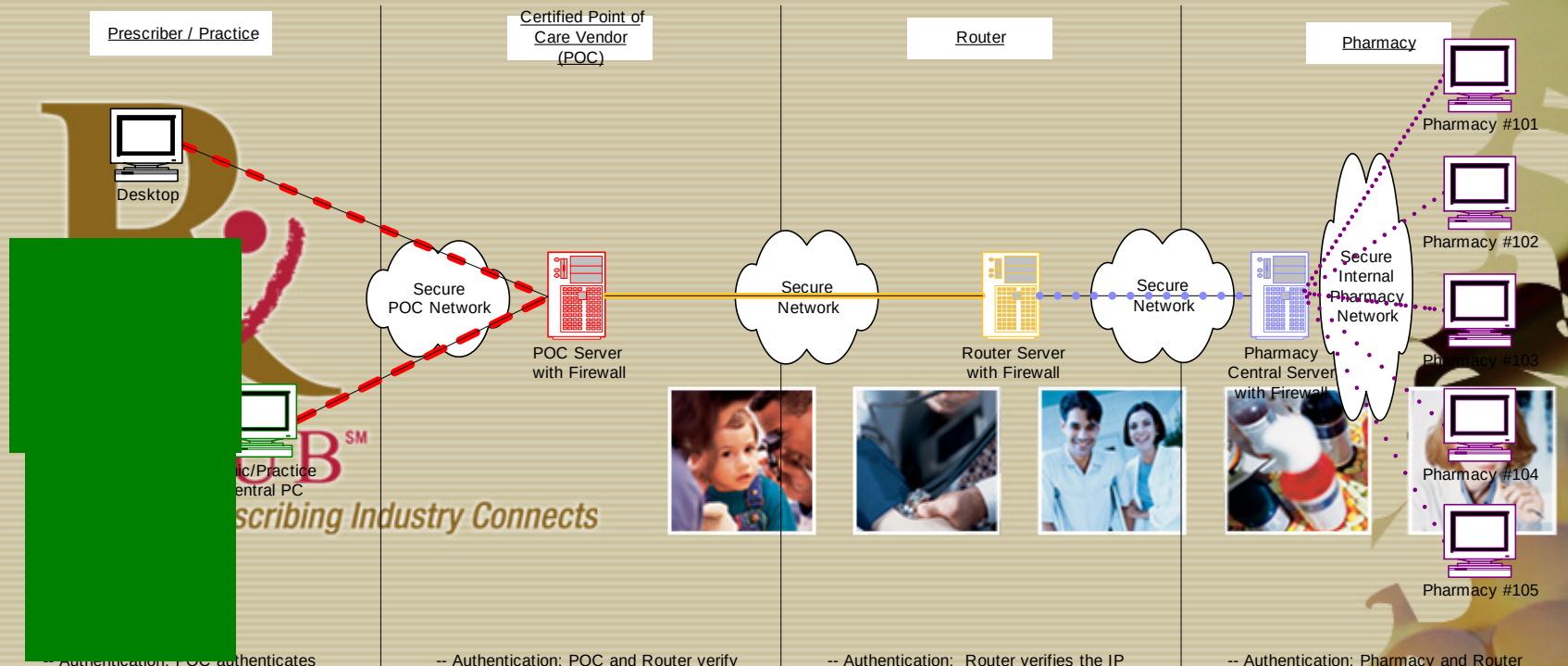
Mark Gingrich, RxHub LLC

July 11, 2006

RxHub Overview

- Founded 2001 as nationwide, universal electronic information exchange
- Encompass five of the largest pharmacy benefits managers (PBMs)
  - CaremarkPCS, Express Scripts, Medco Health Solutions
  - 160 million covered lives (and growing with addition of new participants ~80% commercial market)
  - Pharmacare, Argus
    - Additional 50 million covered lives
- Includes participation by point-of-care technology vendors, electronic medical record vendors, health plans, hospitals, and pharmacies
- Processing over 4.3 million transactions a month that correlate to a point-of-care patient visit
  - 20.5 million incoming eligibility in 1H2006 (26.5M in 2005)
  - 2.2 million med history summaries in 1H2006 (2.5M in 2005)
  - **111 thousand electronic prescriptions in 1H2006 (33K in 2005)**

Electronic Prescribing Security and eSignature Infrastructure



-- Authentication: POC authenticates prescribers before assigning unique IDs to them (IDs are unknown to prescribers).
-- Security: Authenticated prescribers are granted access to POC technology, where they login with unique usernames and passwords.
-- Security: Prescribers send prescription data to POC server through POC's secure channel ( ).
-- Prescribers sign contracts authorizing the POC to act as their authorized agent in sending eRxs.
-- Wireless technologies (e.g. tablet PCs and PDAs) contain their own security profiles to prevent unauthorized access or interception ( ).

-- Authentication: POC and Router verify each other's static IP addresses, IDs and passwords before opening secure channel for transporting an eRx.
-- Security: Prescriber initiates eRx being sent from the POC server to the Router server through the Router's https secure channel ( ).
-- Security: Use of PHI (protected health information) must be in accordance with HIPAA standards for the purpose of treatment, payment or healthcare operations.

-- Authentication: Router verifies the IP addresses, IDs and passwords of each participant (POC and Pharmacy) before opening secure communication channels.
-- Security: Router adheres to security policies which are consistent with HIPAA security guidelines.
-- Security: Router performs internal assessments using security scanning tools for network and system security.
-- Security: Router maintains only enough information to allow for routing, auditing and support.
-- Security: Router may not view or modify eRxs, except when translating from one messenging standard to another (e.g. HL7 to NCPDP).

-- Authentication: Pharmacy and Router verify each other's IP addresses, IDs, and passwords before opening a secure channel ( ) for transporting eRxs.
-- Authentication: Pharmacy stores a cross-reference table containing DEAs and their unique IDs (assigned by POCs).
-- Audit Trail: Pharmacists may contact a POC or prescriber at any time to verify the authenticity of an eRx.
-- Audit Trail: POC, Router and Pharmacy maintain transaction logs that may be used for auditing purposes.
-- Authentication: Pharmacy (Central Server) and each Pharmacy site verify each other's IP addresses, IDs, and passwords before opening a secure channel ( ) for transporting eRxs.

11/16/2004

11/22/2004

RXHUB™
Where the Prescribing Industry Connects

Security: What does HIPAA "require" of a Covered Entity to achieve "Security" of Protected Health Information

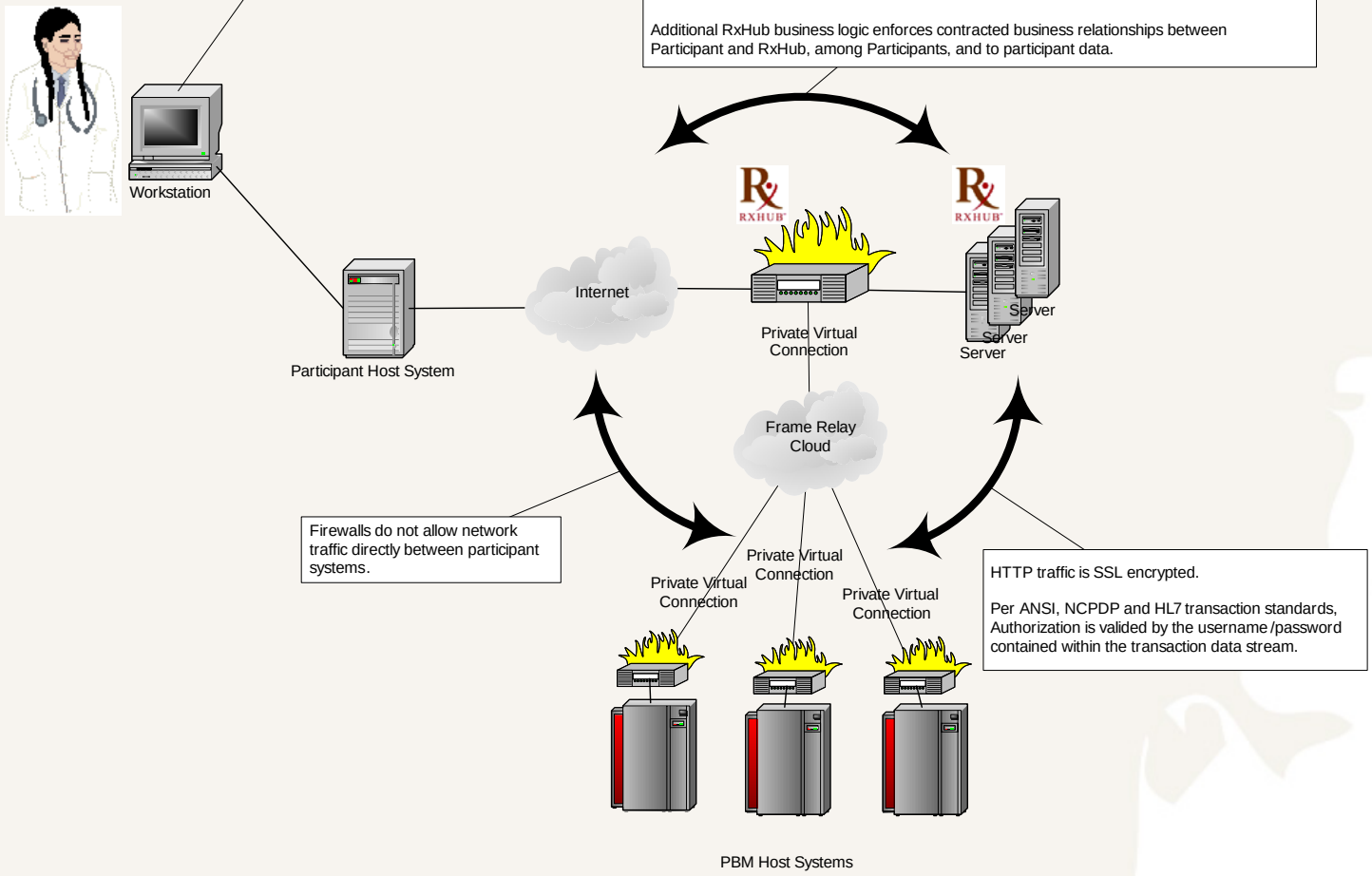
Requirement	Description	eRx
Administrative Safeguards	• prevent, detect, document, contain and correct security violations; • determine appropriate, limited access to be given to identified individuals; • ensure workforce training regarding security policies; • provide planned response to threatening occurrences (natural disasters, vandalism, etc.); • implement periodic technical testing and evaluations.	✓
Physical Safeguards	Appropriately limit physical access to electronic information systems, hardware, software and facilities in which they are housed against unauthorized access.	✓
Technical Safeguards	Implement unique names/numbers to track access; emergency access procedures; audit controls that record and examine system access and activity; protection against improper alteration/destruction; procedures to authenticate user access; measures to protect information being transmitted against unauthorized access or modification without detection. Note: Current industry standard is SSL ("channel encryption"); encryption of data during transmission is "addressable", not "required".	✓
Organizational Safeguards	Enter into Business Associate contracts with all applicable entities obligating them to comply with similar requirements.	✓
Documentation Requirements	Document policies and procedures applicable to the foregoing, including actions taken and assessments made; such documents must be retained for six (6) years, appropriately made available, and reviewed periodically for updates/revisions.	✓

RxHub Practices

- Point Of Care (POC) user authentication and authorization contractually required
- IP Address verification – sender and receiver
- Participant ID and password verification
- Secure encrypted channel
- Transaction audit – Date/time, sender, receiver, control numbers…
- Meets HIPAA requirements for PHI
- Prescriber and pharmacy are identified in the transaction based on the SCRIPT standard
- Provider directory – physician IDs, NCPDP ID, name, address, phone …
- Industry accepted security controls/processes implemented
- RxHub only opens SCRIPT payload for version translation
  - Validates payload
  - Routing only for transactions on same version of NCPDP standard
- Future: translation from HL7 to NCPDP SCRIPT

Note: As secure (if not more) than paper or fax prescriptions

The RxHub Security Architecture



RxHub Security Summary

- Based on the Information Security Forum's "Standard of Good Practice"
- Annual risk assessments & staff security training
- Use of Intrusion Detection System
- Minimal access Firewall policy
- Password Policy & automatic screen lock
- Use of SSL and digital certificates for data in transit
- Daily encrypted backups performed, secure offsite rotation
- "Hardened" Operating Systems
- Data Retention Policy
  - minimum data required to complete transactions
  - data expired/de-identified as appropriate
- Appropriate Use policy for phone, fax, email, computers, internet
- Use of anti-SPAM & antivirus software at PC and email server
- Automated application of Microsoft patches (Win XP, SP2)
- Use of secure document disposal service
- Established Change Management and Problem Management Processes

Electronic Prescribing Issues

- Today some state regulations are inconsistent or unclear
- Prescriptions can be written in a different state than the pharmacy that fills the prescription
- State regulations don't always consider electronic prescribing and in some cases prohibit electronic prescribing
- Pharmacists unsure of how to determine authenticity of an electronic prescription
  - Pharmacists may call prescriber to verify
  - Pharmacist may print and fax the prescription to prescriber for signature
- The definition of "electronic signature" is not clear

Recommendation

- Current standards and ‘best practices’ provide the necessary processes and protections to support electronic prescribing of both controlled and non-controlled substances.
  - Security – systems and procedures
  - POC user authentication and authorization
    - Unique user ID’s and passwords
  - Unique participant ID’s and passwords
  - Secure encrypted channels for communications
  - IP address verification
  - Transaction audits
  - Allow translation between standards and versions